Questionnaire for Cross-Sectional GDPR Examination

1. Preparation for the GDPR

How have you prepared yourself as a company for the GDPR?

Briefly describe the approach, which departments were involved, and what measures were initiated. To the extent that not all [compliance] measures have been fully implemented yet, please also describe the implementation status.

2. Record of Processing Activities

How have you ensured that all business processes in connection with which personal data are processed were included in a record of processing activities? How do you ensure the record is kept up-to-date? Please attach an overview of your documented processing activities, as well as a sample processing activity as an example.

3. Legal Basis of Data Processing

On what legal bases do you process personal data? To the extent that you also process personal data on the basis of consent, please attach your template [consent materials].

4. Data Subject Rights

How do you ensure compliance with the rights of data subjects (to information, access, rectification, erasure, restriction of processing, and data portability)? Outline your relevant processes and in particular, describe in detail how you are fulfilling your information obligations. Please attach any existing template information notices / privacy notices.

5. Technical Data Protection

a. How do you ensure that your technical and organizational measures – and those of your service providers – provide a level of protection appropriate to the risk of processing?

b. How do you ensure that your technical and organizational measures are adapted to the current state of the art?

c. How do you ensure that you have a documented data-protection-compliant role-based and access-rights scheme for your current or future IT applications?

d. How do you ensure that data protection requirements are taken into account from the outset when designing or modifying new products or services (Privacy by Design and by Default)?

6. Data Protection Impact Assessment

a. How do you ensure that processing activities with a high risk to the rights and freedoms of data subjects are identified, and that for such activities a Data Protection Impact Assessment (DPIA) is conducted?

b. In your company, have you identified processing operations that are likely to result in a high risk to the rights and freedoms of data subjects? If so, which operations? Please attach the relevant DPIA documentation.

7. **Data Processors**

   Have you adapted your existing contracts with data processors to the new GDPR requirements? If you use template agreements, please attach them – and also please attach a sample agreement with one of your data processors.

8. **Data Protection Officer**

   How is your Data Protection Officer integrated into your organization? What documented qualifications does he have?

9. **Reporting Obligations**

   How do you ensure that your company reports data protection incidents and violations to the supervisory authority on time? Outline your processes in this regard.

10. **Documentation**

    How can you prove your compliance with all the obligations set forth in points 2-9 above?